WHAT IS CLAIMED IS:

1   1.   A method of sending a packet from a first IPSec client to a second IPSec client,

2   comprising the steps of:

3   receiving at a non-proprietary format tunneling protocol server from the first

4   IPsec client an IPsec packet wrapped in the non-proprietary tunneling format;

5   creating a non-proprietary format tunneling protocol tunnel to the second IPsec

6   client through the non-proprietary format tunneling protocol server;

7   establishing a security association between the first and second IPSec clients via

8   the non-proprietary format tunneling protocol server;

9   transmitting the packet through the non-proprietary format tunneling protocol

10   tunnel to the second IPSec client whereby the packet remains unaffected by any address

11   translation or firewall traversal that may occur during transmission.

1   2.   The method according to claim 1 wherein the non-proprietary tunneling

2   protocol comprises a Layer-2 Tunneling Protocol (L2TP) protocol.

1   3.   The method according to claim 2 wherein the receiving step includes the

2   steps of:

3   opening an LT2P tunnel between the first IP client and the server; and

4   communicating an IPsec packet wrapped in an L2TP format to the server.

1   4.   The method according to claim 2 wherein the receiving step includes the

2   step of routing an IPsec packet wrapped in an L2TP format to the server via a public

3   address.

1   5.   The method according 4 wherein the public address supplied from the

2   server to the first IPsec client.